Technical White Paper

FIVE CRITICAL MISTAKES TO AVOID
When Building Your Next Secure Messaging Solution

12AX7 Logic, LLC
9900 45TH AVE. N. #120
PLYMOUTH, MN 55442
612-236-6754 VOICE
www.12ax7logic.com
January 2022

INTRODUCTION: DOING MORE WITH LESS

The whole world is messaging

Providers of secure messaging solutions are working in a very difficult environment. Since the 1990s messaging apps have become prevalent worldwide, with over 3 billion people averaging as many as 72 messages every 24 hours.[1] This staggering number of billions of messages every day shows how popular this means of communication has become. Currently, all messaging apps use a client-server which enables the user to communicate whether one to one, or one to many.

Sensitive data stored on servers

When users sign up for a service, they are asked to provide sensitive, personal information that is saved to a server including name, phone number, email address, and in some cases, even date of birth and banking or credit card info. This is cause for concern because of server vulnerably to hackers.

Technology remains unchanged

The technology used to connect operations of secure messaging solutions has remained basically unchanged over the last 30 years, with centralized servers used for the flow and storage of critical personal data, messages, and content risking their availability to hackers.

A new perspective

This white paper looks at a new way to develop and deliver a highly secure message solution that supports internal and external users, at an affordable cost. This novel process is a peer-to-peer (P2P) decentralized message connection using Point-to- Point Encryption (P2PE), with messages sent directly from user to user, without using vulnerable intermediary servers.

Cyber Security is National Security

In the past, after providing sensitive, personal data permanently held in a database, the message originator constructs and sends a message, but first it must be sent to the connection server, to make the connection with the recipient.

After queueing the receiver, the server holds the message and any attached media on the server awaiting response. This server involvement is an unnecessary weak link in the system, and where the problems begin.

To help provide security on a messaging app, end-to-end encryption (E2EE) is used with the messages and media files stored on the server, until the receiver gets the message.

As messages currently make their way through centralized servers however, the stored sensitive messages or files, and often the personal identity data of the users, exposes them by default to many risks that of hacked personal data, cybertheft, and violations of privacy.

As cyber threats increase, a movement is growing to decentralize messaging. Messages will be sent directly from user to user without an intermediary with Point-to-Point encryption (P2PE)[3].

1. https://www.trillmag.com/43442/read/news/can-popular-messaging-apps-like-whatsapp-be-hacked/
2. https://www.visualcapitalist.com/evolution-instant-messaging/
3. https://www.pandasecurity.com/en/mediacenter/mobile-news/time-to-dump-whatsapp/
4. https://www.fedscoop.com/bill-to-create-cybersecurity-workforce-rotational-program-passes-house/
5. https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en#top-of-page
6. https://medium.com/ieeeditu/end-to-end-encryption-4e9b67827d17
7. https://www.foregenix.com/blog/p2pe-what-are-the-benefits-to-retail-merchants
8. https://www.gomyitguy.com/blog-news-updates/point-to-point-vs-end-to-end-encryption#:
9. https://www.indianadscompany.com/fedramp-certification-what-is-it-why-it-matters-and-who-has-it/

Managing today's complex security threats using messaging solutions has become more difficult than ever.

Today personal information is gold. Because of the popularity with secure messaging, it has attracted a darker side to infiltrate and attack any potentially vulnerable weak links. These targets for cyber-attacks include personal sensitive information that are permanently stored on servers, along with any undelivered text and media files on servers typically stored for up to 30 days, maybe longer, during attempted delivery.

Weak links are cyber-attack opportunities

In this mobile society, so-called "secure" messaging solutions are constantly under attack. Secure messaging solutions like WhatsApp the world's number one most popular messaging app, are popular because it is believed they are safe, no one can read your messages or access personal data or attached files except for you, right? Unfortunately, that's not true, messaging app databases can be hacked![2] By storing this sensitive personal information, a glaring weakness is exposed.[4] Even with E2EE, all cyber-attacks where critical information and data were breached, stolen, or otherwise compromised, they have one thing in common they employed a server in the middle with E2EE that was hacked.

What is the weak link?

As designed over 30 years ago with the available technology at the time, it is the server that holds sensitive personal information and establishes the connection to make everything happen. The more computer **servers used** to hold user data and make connections - the more computer **server opportunities** there are for a cyber-attack.

Increasing use of weak links increases Cyber security threats

As written by Jackson Barnett on September 29, 2021, in FEDSCOOP; Rep. Nancy Mace, R-S.C., co-sponsored the House version of a bill that would set up a cybersecurity workforce rotational program that passed the House of Representatives with bipartisan support.[5] The bill comes after high-profile cyberattacks against the government, like the SolarWinds hack, have increased the urgency of lawmakers attempting to help agencies recruit and retain cyber talent. *"Cyber security is national security."* Mace said in a statement. *"In fact, just last year 11 federal agencies were hacked by a group affiliated with Russia. Our cyber security challenges are dramatically increasing."*

E2EE doesn't eliminate the weak link

To help provide better security, providers of secure messaging solutions have tried to address this cumbersome and complex system with the security measure called End-to-End Encryption (E2EE).

This attempts to protect data and files with encryption passing through a server that must be used to initiate, facilitate, and complete the actual connection between devices. However, this approach does not stop hackers. For messaging apps, the weak "LINK" is the "SERVER" in the middle - that must "ESTABLISH" the connection of the two devices.

1. https://www.trillmag.com/43442/read/news/can-popular-messaging-apps-like-whatsapp-be-hacked/
2. https://www.visualcapitalist.com/evolution-instant-messaging/
3. https://www.pandasecurity.com/en/mediacenter/mobile-news/time-to-dump-whatsapp/
4. https://www.fedscoop.com/bill-to-create-cybersecurity-workforce-rotational-program-passes-house/
5. https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en#top-of-page
6. https://medium.com/ieeeditu/end-to-end-encryption-4e9b67827d17
7. https://www.foregenix.com/blog/p2pe-what-are-the-benefits-to-retail-merchants
8. https://www.gomyitguy.com/blog-news-updates/point-to-point-vs-end-to-end-encryption#:
9. https://www.indianadscompany.com/fedramp-certification-what-is-it-why-it-matters-and-who-has-it/

This guide can help

While every project has its challenges, this common-sense guide presents five mistakes we see repeatedly, along with tips on how to avoid each one. We hope this guide will help you to create a new secure messaging solution that meets all your goals providing a dependable way to communicate free of cyber espionage concerns.

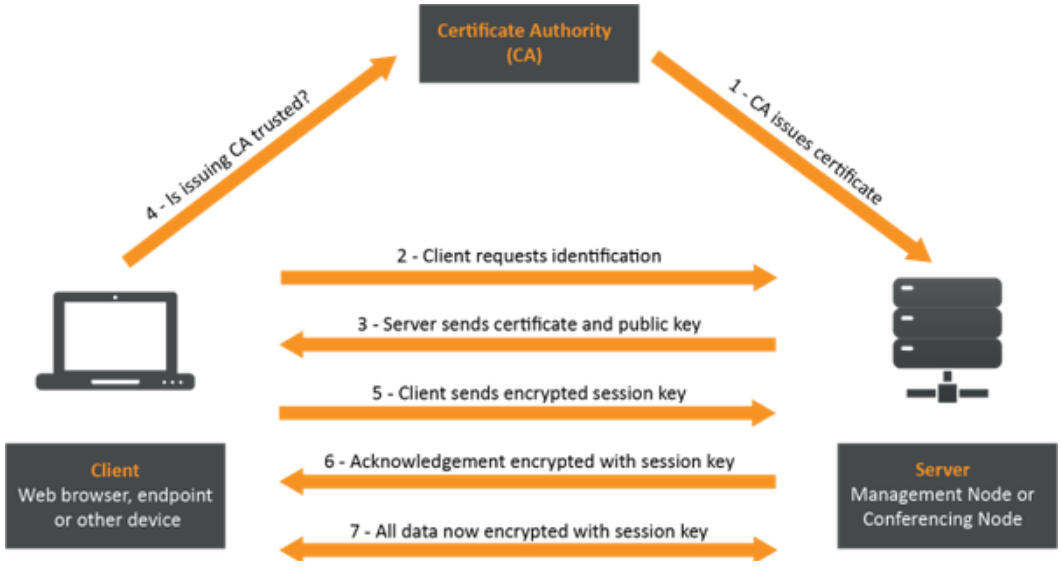
MISTAKE 1: Using the Industry Standard Client-Server Method

Currently, the approach to constructing common secure messaging solutions is known as a client-server method, which enables a user to communicate. This method obtains the security E2EE standards that helps secure and alleviate concerns of cyber espionage. But there are good reasons to rethink this approach.

Valuable data held means time is not on your side

Although E2EE is a secure protocol, the user who wants to send a message, first sends the text or media file to the server. Then the server queues the message on the receiving number and device when they have an internet connection. Once the receiver connects and retrieves the text and/or media file, the server instantly removes them. This helps the server to keep resources to the minimum. The transfer of data on all common wireless messaging solutions is end-to-end encrypted. This means the server can't decode and won't store the messages after delivery. The messages are only decoded when the receiver gets the message.

Client-Server Connection

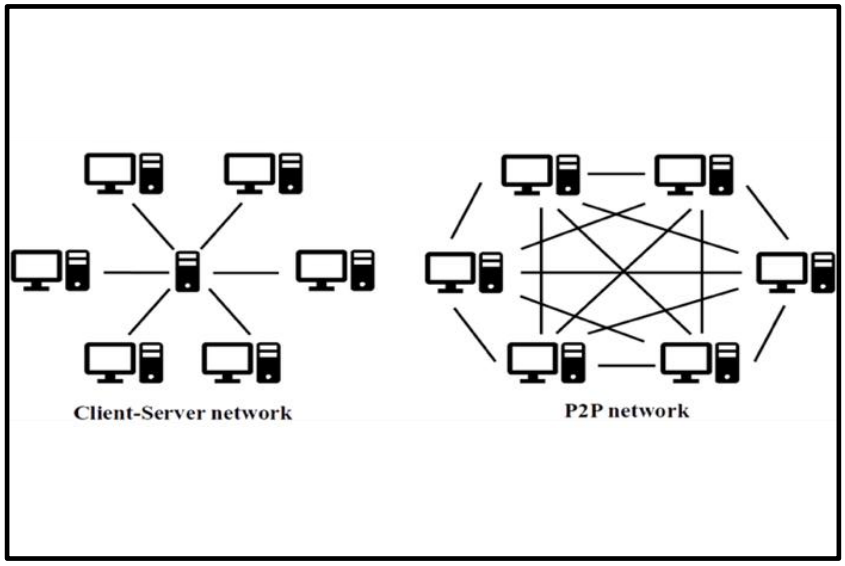


However, using this server to make the connection between users of Secure messaging, is a critical mistake. As compared to a Peer-to-Peer (P2P) connection, (more on this later), this not only adds an unnecessary database of critical information potentially vulnerable to cyber threats, but it also increases the opportunities for bad actors to infiltrate the connection between the two users, such as using a Man in the Middle (MitM) cyber-attack.

1. https://www.trillmag.com/43442/read/news/can-popular-messaging-apps-like-whatsapp-be-hacked/
2. https://www.visualcapitalist.com/evolution-instant-messaging/
3. https://www.pandasecurity.com/en/mediacenter/mobile-news/time-to-dump-whatsapp/
4. https://www.fedscoop.com/bill-to-create-cybersecurity-workforce-rotational-program-passes-house/
5. https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en#top-of-page
6. https://medium.com/ieeeditu/end-to-end-encryption-4e9b67827d17
7. https://www.foregenix.com/blog/p2pe-what-are-the-benefits-to-retail-merchants
8. https://www.gomyitguy.com/blog-news-updates/point-to-point-vs-end-to-end-encryption#:
9. https://www.indianadscompany.com/fedramp-certification-what-is-it-why-it-matters-and-who-has-it/

Client-Server Network Comparison to Peer-to-Peer Network

The illustration below of the client-server network as compared to a peer-peer (P2P) network, clearly illustrates the profound increase in security of P2P connection, with the absence of a server used to make connections. When a connection is set up directly from one secured wireless device directly to another secured wireless device, a dramatic reduction in opportunities for cyber threats is achieved in sharing encrypted data and media. Although E2EE encryption is known to be secure with the client-server architecture, the ability of have a highly functioning secure messaging solution, with the least number of computer components working with each other, is clearly an advantage obtained with a secure peer-to-peer connection, as compared with the added server needed in a client-server model.



Beware of Who or "What's" Behind the Curtain

As a further example of a potential weakness of the client-server method, at its launch in 2009, WhatsApp was designed to be a simple messaging app that would allow anyone, anywhere to send text messages to their contacts. Facebook bought WhatsApp in 2014, but at its core, Facebook is an advertising company, building extremely detailed profiles about each of its users, for targeted ads based on their preferences. Originally, WhatsApp users could opt out of data sharing. But from the beginning of this last February, the opt out has been removed and there is nothing you can do to prevent Facebook accessing your account information[4].

CONCLUSION: Reduce the ability of bad actors to access important data.

1. https://www.trillmag.com/43442/read/news/can-popular-messaging-apps-like-whatsapp-be-hacked/
2. https://www.visualcapitalist.com/evolution-instant-messaging/
3. https://www.pandasecurity.com/en/mediacenter/mobile-news/time-to-dump-whatsapp/
4. https://www.fedscoop.com/bill-to-create-cybersecurity-workforce-rotational-program-passes-house/
5. https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en#top-of-page
6. https://medium.com/ieeeditu/end-to-end-encryption-4e9b67827d17
7. https://www.foregenix.com/blog/p2pe-what-are-the-benefits-to-retail-merchants
8. https://www.gomyitguy.com/blog-news-updates/point-to-point-vs-end-to-end-encryption#:
9. https://www.indianadscompany.com/fedramp-certification-what-is-it-why-it-matters-and-who-has-it/

MISTAKE 2: Not Providing Complete Anonymity

A secure messaging solution with users' identity listed in a database is a key security concern. The problem is all current client-server models of secure messaging solutions require keeping the name, phone number, and sometimes even more personal information in a server about each user. But there are good reasons to rethink this approach.

Requiring too much real information

With most current message solutions such as WhatsApp, the user who wants to send a message, must accept a concerning fact, that multiple aspects of their identity are stored in a database[6]. The use of ubiquitous client-server architecture used in all popular secure messaging solutions requires user identity data which, when saved and stored on a server supplies an attractive target for cyber-attacks from bad actors.

CONCLUSION: Don't Divulge User Identity

MISTAKE 3: Storing Something Valuable to Steal

A secure messaging solution with valuable user data and media files even temporarily stored in a database is a key security concern. The problem with all current client-server models of secure messaging solutions is, the vast amount of required key user data and temporarily held while awaiting connection[5] even media files, which can be solen from a centralized server. But there are good reasons to rethink this approach.

Requiring too much information to be held

With most current message solutions such as WhatsApp, the user who wants to send a message, must accept a concerning fact that to use the service, extensive user information is held in a database[6]. This can include among others:

- Usage and Log Information
- Device and Connection Information
- Location Information
- Cookies
- Information Others Provide About You
- User Reports
- Third-Party Service Providers
- Third-Party Service

As previously shown, for the last 30 years the seemingly antiquated use of the ubiquitous client-server architecture requiring retention of key sensitive data and media, supplies fertile ground for cyber-attacks in all popular secure messaging solutions. Again, the obvious answer is to end the need for keeping personal, and other vital files or information on a potentially vulnerable centralized server, to help decrease or stop cyber threats.

CONCLUSION: Centralized Data and File Retention are Cyber Threats

1. https://www.trillmag.com/43442/read/news/can-popular-messaging-apps-like-whatsapp-be-hacked/
2. https://www.visualcapitalist.com/evolution-instant-messaging/
3. https://www.pandasecurity.com/en/mediacenter/mobile-news/time-to-dump-whatsapp/
4. https://www.fedscoop.com/bill-to-create-cybersecurity-workforce-rotational-program-passes-house/
5. https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en#top-of-page
6. https://medium.com/ieeeditu/end-to-end-encryption-4e9b67827d17
7. https://www.foregenix.com/blog/p2pe-what-are-the-benefits-to-retail-merchants
8. https://www.gomyitguy.com/blog-news-updates/point-to-point-vs-end-to-end-encryption#:
9. https://www.indianadscompany.com/fedramp-certification-what-is-it-why-it-matters-and-who-has-it/

MISTAKE 4: Incorrectly Assuming E2EE is Safe and Secure

WHAT IS End-to-End ENCRYPTION (E2EE)?

E2EE is the process of encrypting data being passed through a network however, the routing information stays visible.

ADVANTAGES OF E2EE

End-to-end encryption (E2EE) is the most used encryption standard for secure communication[7]. Advantages of E2EE are it ensures the privacy of our data that we share through the internet using different platforms, and makes it nearly impossible to corrupt messages, documents, and voice messages.

THREATS TO E2EE:

Despite these advantages, E2EE has some distinct disadvantages and threats too.

- Smartphones are a common medium of communication and hold a huge amount of our data in plaintext. However, E2EE does not secure endpoint communication. Any cyber-attacks on our smartphones, E2EE will not be able to help.
- E2EE uses public-key cryptography, meaning a secret key and a public key, are both shared with anyone. However, E2EE does not verify to ensure that your device is communicating with the intended receiver's device. That verification is necessary to ensure that there is no man in the middle attack (MitM) in between.

WHAT IS Point-to-Point ENCRYPTION (P2PE)?

"Point-to-point encryption (P2PE) is the secure encrypting of transacted data through a designated "tunnel". Traditionally, P2PE is most often applied to credit card information encrypted from the merchant point-of-sale (POS) entry to the final credit card processing point. However, the principle of P2PE technology is that it can protect sensitive data in many ways.

ADVANTAGES OF P2PE:

Point-to-Point-Encryption, known to most as P2PE is a standard that is quickly becoming the preferred way for acquirers and merchants to secure customer cardholder data[8]. Developed in 2012 after some large-scale, high-profile credit card data hacks, P2P simplifies and hardens how the value chain of in-person payment works for Retailers worldwide. P2PE is considered the benchmark standard for the encryption of credit card payment data within a secure environment using industry standard cryptographic algorithms.

THREATS TO P2PE:

Despite these advantages, P2PE has some distinct disadvantages and threats too[8]. The need for better security is becoming a major theme in business and government IT. Within P2PE a common retailer standard caused a controversy after some notable data breaches from inside big-retailer systems. Due to in-adequate compliance measures, there was a data breach. It makes a difference as the breached data was not stolen in the "tunnel" but when it was at rest, stored on a server for future use in networks.

1. https://www.trillmag.com/43442/read/news/can-popular-messaging-apps-like-whatsapp-be-hacked/
2. https://www.visualcapitalist.com/evolution-instant-messaging/
3. https://www.pandasecurity.com/en/mediacenter/mobile-news/time-to-dump-whatsapp/
4. https://www.fedscoop.com/bill-to-create-cybersecurity-workforce-rotational-program-passes-house/
5. https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en#top-of-page
6. https://medium.com/ieeeditu/end-to-end-encryption-4e9b67827d17
7. https://www.foregenix.com/blog/p2pe-what-are-the-benefits-to-retail-merchants
8. https://www.gomyitguy.com/blog-news-updates/point-to-point-vs-end-to-end-encryption#:
9. https://www.indianadscompany.com/fedramp-certification-what-is-it-why-it-matters-and-who-has-it/

Those organizations that push end-to-end encryption as part of their solutions (to sell more), often claim E2E encryption is safer than P2P encryption. However, evidence clearly shows that P2P encryption seems to be better from a security standpoint[8]. With E2E's required connection point **C** between systems **A** and **B,** that connection point easily may increase the chance of hacking.

CONCLUSION: Choose P2PE Rather Than E2EE for More Secure Architecture

MISTAKE 5: Not Having FedRAMP Certification

There are four impact levels FedRAMP offered for services with different kinds of risk, based on the potential impacts of a security breach in three different areas[9]. ("FedRAMP Certification: What Is It, Why It Matters, and Who ...") The three areas are:

A. **Confidentiality:** Protections for privacy and proprietary information.
B. **Integrity:** Protections against modification or destruction of information.
C. **Availability:** Timely and reliable access to data.

The four impact levels are[9]:

1. **High, based on 421 controls.** "The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals." ("FIPS 199, Standards for Security Categorization of Federal ...") "This usually applies to law enforcement, emergency services, financial, and health systems.
2. **Moderate, based on 325 controls.** "The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals." ("FIPS 199, Standards for Security Categorization of Federal ...") "Nearly 80 percent of approved FedRAMP applications are at the moderate impact level."
3. **Low, based on 125 controls.** "The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals."
4. **Low-Impact Software-as-a-Service (LI-SaaS), based on 36 controls**. For "systems that are low risk for uses like collaboration tools, project management applications, and tools that help develop open-source code." This category is also known as FedRAMP Tailored.

1. https://www.trillmag.com/43442/read/news/can-popular-messaging-apps-like-whatsapp-be-hacked/
2. https://www.visualcapitalist.com/evolution-instant-messaging/
3. https://www.pandasecurity.com/en/mediacenter/mobile-news/time-to-dump-whatsapp/
4. https://www.fedscoop.com/bill-to-create-cybersecurity-workforce-rotational-program-passes-house/
5. https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en#top-of-page
6. https://medium.com/ieeeditu/end-to-end-encryption-4e9b67827d17
7. https://www.foregenix.com/blog/p2pe-what-are-the-benefits-to-retail-merchants
8. https://www.gomyitguy.com/blog-news-updates/point-to-point-vs-end-to-end-encryption#:
9. https://www.indianadscompany.com/fedramp-certification-what-is-it-why-it-matters-and-who-has-it/

The ability to achieve FedRAMP certification is very difficult for a commercial secure messaging solution with E2EE security, using the typical server-in-the-middle-connection to hold sensitive personal, shared data, and media, as the process of achieving FedRAMP authorization can be tough. Interestingly, only Slack, Trello, and Zendesk are FedRAMP certified, with Slack having only a Moderate impact level rating, with both Trello and Zendesk having the lowest Low-Impact level rating, and Zendesk is not even offering end-to-end encryption. Interestingly to note, at this time, no secure messaging solution using Point-to-Point Encryption has applied for FedRAMP certification.

CONCLUSION: No Current Messaging Solutions are High FedRAMP Certified

About 12AX7 Logic:

12AX7 Logic, LLC is a Plymouth, Minnesota-based software company founded in October of 2018. The company was originally formed to provide professional software and related full software-as-a-service (SaaS) components to government defense agencies, and the law enforcement market. As the changing market forces dictated by COVID-19 impacted potential clients' needs, so did 12AX7 Logic's services expansion of their client services to include secure audio and video communication services along with encrypted**,** direct wireless messaging and file-sharing capabilities, for federal and state government, law enforcement, specialized legal firms, wealth management, higher education, and high net-worth individuals in professional sports and entertainment.

We use this expertise to produce the first, patented, secure, direct, Peer-to-Peer messaging system with Point-to-Point (P2P) encrypted, data-sharing technology sent from one wireless mobile device directly to another wireless mobile device, through a computer interface, over a secured or unsecured DoD or other highly secure network, or supported cellular Network via the Internet.

The first two applicational uses produced with this groundbreaking technology with five awarded patents provide a private, invitation-only, encrypted, communication network directly connecting mobile device users in a secure membership circle. This membership circle network enables users the connection and transfer of secure, bank-level encrypted data and all file formats, sent directly between wireless devices through a choice of multiple communication channels including, Bluetooth, WiFi Direct, and the Internet. This highly secure private communication network includes instant messaging, emailing with encrypted attachment, secure audio and video calling, and encrypted file sharing on, private-cloud-based software-as-a-service (SaaS) mobile apps, **PENTODE®** and **TETRODE®**. 12AX7 Logic feels this is the better way to accomplish this secure communication goal.

For more information contact info@12ax7logic.com or visit www.12ax7logic.com.

1. https://www.trillmag.com/43442/read/news/can-popular-messaging-apps-like-whatsapp-be-hacked/
2. https://www.visualcapitalist.com/evolution-instant-messaging/
3. https://www.pandasecurity.com/en/mediacenter/mobile-news/time-to-dump-whatsapp/
4. https://www.fedscoop.com/bill-to-create-cybersecurity-workforce-rotational-program-passes-house/
5. https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en#top-of-page
6. https://medium.com/ieeeditu/end-to-end-encryption-4e9b67827d17
7. https://www.foregenix.com/blog/p2pe-what-are-the-benefits-to-retail-merchants
8. https://www.gomyitguy.com/blog-news-updates/point-to-point-vs-end-to-end-encryption#:
9. https://www.indianadscompany.com/fedramp-certification-what-is-it-why-it-matters-and-who-has-it/